IN THE CLAIMS:

1. (Currently amended) A method for documenting a transfer of authority of control for a container from a first entity of a transportation chain to a second entity of the transportation chain, the method comprising:

receiving through ~~in~~ an interface of an electronic seal associated with the container an electronic container control certificate associated with a first entity, the electronic seal including a log for recording data and a control unit for verifying data received through the interface, the electronic container control certificate comprises a cryptographic key associated to the second entity, and which container control certificate is digitally signed by the first entity; ~~and~~

receiving in the electronic seal associated with the container, geographic location data from a location recording device associated with one of the first and second ~~entities~~ entities;

storing the container control certificate in the log of the electronic seal; and

verifying the signed container control certificate by a corresponding function implemented in the electronic seal.

2. (Cancelled)

3. (Cancelled)

4. (Original) Method according to claim 3, comprising verifying the digital signature of the container control certificate by applying decrypt information stored in the log of the electronic seal and delivered to the log by a previous entity of the transportation chain.

5. (Original) Method according to claim 4, wherein the verification is considered to be failed if the signed container control certificate cannot be decrypted with the decrypt information stored in the log.

6. (Previously presented) Method according to claim 3, wherein a status of a container lock is subject to the result of the signature verification process.

7. (Previously presented) Method according to claim 3, wherein the electronic seal issues a warning if the verification of the signature fails.

8. (Previously presented) Method according to claim 3, wherein the container control certificate is stored in the log if the verification succeeds.

9. (Previously presented) Method according to claim 1, wherein the cryptographic key associated to the second entity is used by the electronic seal for decrypting data expected to be received from the second entity.

10. (Previously presented) Method according to claim 1, wherein the electronic seal is designed for controlling a lock of the container.

11. (Previously presented) Method according to claim 1, wherein an asymmetric cryptographic key system is used for digitally signing the container control certificate.

12. (Original) Method according to claim 11, wherein a public--private key system is used for digitally signing the container control certificate.

13. (Original) Method according to claim 12, wherein the container control certificate is signed using a private key associated to the first entity.

14. (Previously presented) Method according to claim 4, wherein the container control certificate is signed using a private key associated to the first entity and the decrypt information stored in the log comprises a public key of the first entity.

15. (Previously presented) Method according to claim 1, wherein the first entity receives the cryptographic key associated to the second entity from a certificate authority.

16. (Previously presented) Method according to claim 1, wherein the container control certificate comprises identification data for the container.

17. (Cancelled)

18. (Previously presented) Method according to claim 1, wherein the location data is digitally signed by the associated entity.

19. (Previously presented) Method according to claim 1, wherein the signed location data is stored in a log of the electronic seal.

20. (Previously presented) Method according to claim 1, comprising verifying the signed location data by a corresponding function implemented in the electronic seal.

21. (Original) Method according to claim 20 comprising verifying the digital signature of the location data by applying decrypt information stored in the log of the electronic seal and delivered to the log by a previous entity of the transportation chain.

22. (Previously presented) Method according to claim 20, wherein the verification is considered to be failed, if the signed location data cannot be decrypted with decrypt information stored in the log.

23. (Previously presented) Method according to claim 20, wherein recording the location data in the log of the electronic seal is subject to a result of the signature verification process.

24. (Previously presented) Method according to claim 1, wherein the electronic seal transmits container identification information to a location recording device associated to one of the entities.

25. (Previously presented) Method according to claim 24, wherein the transmitted container identification information is digitally signed by a second entity.

Claims 26-28 (Cancelled)

29. (Original) Computing unit according to claim 18, comprising a log for storing a cryptographic key associated to the certificate authority for decrypting information received from the certificate authority via the certificate authority interface.

Claims 30-70 (Cancelled)